Japanese Laid-open Application Publication No. 11-212849 (D4)

The invention of D4 relates to the shared file transmission and reception system provided with the access control function. ([0001])

The invention of D4 makes the list that describes conditions of a user to allow the access as the conditional equation combined with the attribute information of the user, and stores the shared file added this in the server information processor. It is constructed to acquire the login information of the user who tries to access to it by the client information processor, and based on the list added to the shared file to be accessed, judge the access right by the access right discrimination processor, and send the shared file from the server information processor to the client information processor according to this discrimination. (Abstract)

cited reference④

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－212849

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/00	５３７	Ｇ０６Ｆ　12/00	５３７Ａ

審査請求　未請求　請求項の数20　ＯＬ　（全 21 頁）

(21)出願番号　特願平10－16280

(22)出願日　平成10年(1998)１月29日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(71)出願人　000153524
株式会社日立情報ネットワーク
東京都品川区南大井六丁目26番３号

(72)発明者　鍛　忠司
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　荒井　正人
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　共有ファイル送受信システム、アクセス権利判定装置

(57)【要約】

【課題】　共有ファイルへのアクセス権の設定を、ファイルサーバに依らず共通の処理で、かつ、ファイルサーバにおけるアクセス権利設定のための特権を要求することなく行う。

【解決手段】　アクセスを許可するユーザーの条件を、ユーザーの属性情報を組み合わせた条件式として記述したリストが付加された共有ファイルをサーバ情報処理装置１１に格納し、アクセスしようとするユーザーのログイン情報をクライアント情報処理装置１２で取得し、前記ユーザーのログイン情報およびアクセスしようとする共有ファイルに付加されたリストに基づいてアクセス権利判定処理装置１４によりアクセス権利を判定し、この判定に従って共有ファイルを、サーバ情報処理装置１１からクライアント情報処理装置１２にデータ中継装置１３により中継する。

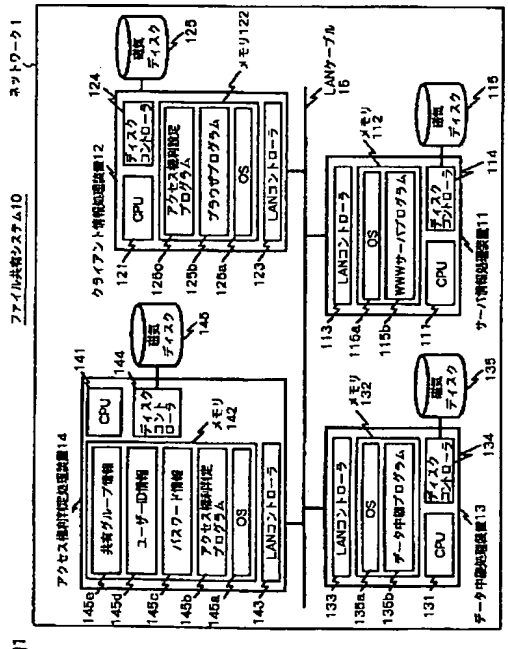


図1

1

【特許請求の範囲】

【請求項１】通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、

共有ファイルにアクセスする権利をデータ受信側の利用者が有するか否かを判定するためのアクセス権利判定手段と、

データ送信側の端末からデータ受信側の端末にファイルを転送するためのデータ中継手段とを備え、

前記共有ファイルは、アクセス権利を持つ利用者を示す開示先情報が予め付加され、

前記アクセス権利判定手段は、共有ファイルにアクセスする権利をデータ受信側の利用者が持つか否かを、当該共有ファイルに付加されている前記開示先情報に基づいて判定し、

前記データ中継手段は、前記データ受信側の利用者の要求に応じてデータ送信側の端末から共有ファイルを受信し、当該受信した共有ファイルに対するアクセス権利を前記利用者が有すると前記アクセス権利判定手段が判定した場合にのみ、前記受信した共有ファイルをデータ受信側の端末に送信することを特徴とする共有ファイル送受信システム。

【請求項２】　請求項１記載の共有ファイル送受信システムにおいて、

前記開示先情報は、それが付加されている共有ファイルに対してアクセスが許可される条件が、個人に関する予め定められた属性情報を指定するリストとして記述され、

前記アクセス権利判定手段は、データ受信側の前記利用者に関する属性情報が前記リストの条件を満足する場合に、前記共有ファイルにアクセスする権利があるものと判断することを特徴とする共有ファイル送受信システム。

【請求項３】　請求項２記載の共有ファイル送受信システムにおいて、

前記リストは、当該リストを識別するための名称が予め定められ、

前記共有ファイルは、前記リストに代えて、当該リストを示す名称が付加され、

前記アクセス権利判定手段は、前記リストと当該リストの名称との組を保持していて、

前記名称に対応する前記リストの条件を前記利用者に関する属性情報が満足する場合に、前記共有ファイルにアクセスする権利があると判断するものであることを特徴とする共有ファイル送受信システム。

【請求項４】　請求項２および３のいずれか一項記載の共有ファイル送受信システムにおいて、

前記共有ファイルには、前記利用者がアクセス権利を持たないことを通知するメッセージが付加されていて、

前記データ中継手段は、前記利用者が前記共有ファイルに対してアクセスする権利を持たないことが、前記アクセス権利判定手段により判断された場合、データ受信側の前記端末に、前記利用者がアクセス権利を持たないことを通知するメッセージを送信することを特徴とする共有ファイル送受信システム。

2

【請求項５】　請求項４記載の共有ファイル送受信システムにおいて、

前記利用者がアクセスする権利を持たないことを通知するメッセージは、データ送信側の前記端末にエラーメッセージファイルとして格納されていて、

前記共有ファイルには、前記メッセージに代えて前記エラーメッセージファイルを示すリンク情報が付加されていて、

前記データ中継手段は、前記利用者が前記共有ファイルに対してアクセスする権利を持たないことが、前記アクセス権利判定手段により判断された場合、データ送信側の前記端末から前記エラーメッセージファイルを受信し、データ受信側の前記端末に前記エラーメッセージファイルを送信することを特徴とする共有ファイル送受信システム。

【請求項６】通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、

アクセスする権利を判定するためのアクセス権利判定装置と、データ受信側の前記端末に前記データを送信するデータ中継装置とが通信回線を介して接続され、

前記アクセス権利判定装置は、

前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わせられて記述されたリストを基に、データ受信側の前記端末の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定し、

前記データ中継装置は、

データ送信側の端末から前記共有ファイルを受信し、

当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、

前記利用者に当該共有ファイルに対するアクセス権利があると前記アクセス権利判定装置が判定した場合にのみ、データ受信側の前記端末に前記データを送信することを特徴とする共有ファイル送受信システム。

【請求項７】共有ファイルを格納するための機能、および、転送要求を受けた共有ファイルを転送するための機能を有するサーバ装置と、

前記サーバ装置から共有ファイルを受信するための機能、および、ユーザーに共有ファイルの情報を表示するための機能を有するクライアント装置と、

共有ファイルの転送要求を前記クライアント装置から前記サーバ装置に中継し、共有ファイルを前記サーバ装置から前記クライアント装置に中継するための機能、および、当該共有ファイルをキャッシュするためのキャッシ

ュ機能を有する代理サーバ装置と、
前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わせられた記述されたリストを基に、前記クライアント装置の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定するためのアクセス権利判定装置と、
前記サーバ装置から前記共有ファイルを受信し、当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、前記アクセス権利判定装置が前記利用者に当該共有ファイルに対するアクセス権利があると判定した場合にのみ、前記代理サーバ装置に前記データを送信するデータ中継装置とが通信回線を介して接続されていることを特徴とする共有ファイル送受信システム。
【請求項８】通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、
通信回線を介して受信する前記情報は、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストであって、
アクセス権利を持つか否かの判断を依頼した依頼者を特定するための依頼者認証手段と、
当該アクセス権利判定装置が管理する前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するためのアクセス権利判定手段とを備えることを特徴とするアクセス権利判定装置。
【請求項９】　請求項８記載のアクセス権利判定装置において、
アクセスを許可する利用者の条件を記述したリストと当該リストの名称との組を記録するための手段と、
前記リストの名称から前記リストを検索するための手段とを備え、
通信回線を介して受信される前記リストには、前記共有リストの名称が含まれ、
前記アクセス権利判定手段は、前記共有リストに前記依頼者に関する情報が含まれている場合にも、アクセスする権利を持つと判断することを特徴とするアクセス権利判定装置。
【請求項１０】通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、
通信回線を介して受信する情報とは、前記依頼者の属性情報を、暗号鍵と呼ばれる情報によって暗号化したものと、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストとであって、
当該アクセス権利判定装置は、前記暗号化された属性情報を、前記依頼者が当該アクセス権利判定装置に登録した、復号鍵と呼ばれる情報によって復号する属性情報復

号手段を備え、
前記アクセス権利判定手段は、前記属性情報復号手段によって復号化した、前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するものであることを特徴とするアクセス権利判定装置。
【請求項１１】　請求項８、９および１０のいずれか一項記載のアクセス権利判定装置において、
前記依頼者認証手段は、ログイン証明書と呼ばれる情報を受信することによって依頼者を特定するものであり、
当該アクセス権利判定装置は、前記ログイン証明書を発行する証明書発行手段を備えることを特徴とするアクセス権利判定装置。
【請求項１２】　請求項１１記載のアクセス権利判定装置において、
前記ログイン証明書には、前記依頼者の識別子と、当該ログイン証明書が有効か否かを調べるための情報と、が記録されていて、
当該アクセス権利判定装置は、受信した前記ログイン証明書が有効か否かを調べる有効性確認手段を備え、
前記依頼者認証手段は、前記ログイン証明書が前記有効性確認手段によって有効であると判断された場合には、前記依頼者の識別子によって依頼者を特定するものであることを特徴とするアクセス権利判定装置。
【請求項１３】　請求項１２記載のアクセス権利判定装置において、
受信したログイン証明書を保存するためのログイン証明書保存手段を備え、
前記有効性確認手段は、新たに受信したログイン証明書が、既に保存されている場合には、当該ログイン証明書が無効であると判定することを特徴とするアクセス権利判定装置。
【請求項１４】請求項１２および１３のいずれか一項記載のアクセス権利判定装置において、
前記ログイン証明書には、当該ログイン証明書の発行日時が記録されていて、
前記有効性確認手段は、現在の日時が、前記許可証の発行日時から所定の期間以上経過している場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。
【請求項１５】　請求項１２、１３および１４記載のアクセス権利判定装置において、
前記ログイン証明書には、当該ログイン証明書を、最も最近に受信した日時が記録されていて、
前記有効性確認手段は、現在の日時が、前記受信日時から所定の期間以上経過している場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。
【請求項１６】　請求項１２から１５のいずれか一項記載のアクセス権利判定装置において、
前記ログイン証明書には、当該ログイン証明書を受信し

た回数が記録されていて、
前記有効性確認手段は、前記受信回数が、所定の回数を超過している場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。
【請求項１７】請求項１２から１６のいずれか一項記載のアクセス権利判定装置において、
前記ログイン証明書には、当該証明書を送信可能な回数が記録されていて、
前記有効性確認手段は、前記送信可能な回数が、所定の回数よりも少ない場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。
【請求項１８】請求項１２から１７のいずれか一項記載のアクセス権利判定装置において、
前記依頼者認証手段は、前記有効性確認手段によって、前記証明書が無効であると判断された場合に、他の認証手法によって前記依頼者を特定するものであって、
前記証明書発行手段は、前記他の認証手法によって依頼者が特定された場合に、証明書を発行するものであることを特徴とするアクセス権利判定装置。
【請求項１９】共有ファイルに対するアクセス権利を持つか否かをコンピュータを用いて判定するためのアクセス権利判定プログラムを格納した記憶媒体において、
共有ファイルを要求しているユーザーが、ログインしているクライアント情報情報処理装置から、当該ユーザーのログイン情報を取得し、
上記ユーザーが要求している共有ファイルを、サーバー情報処理装置から取得し、
上記取得した共有ファイルに付加されている開示先リストに示されている条件を、上記取得したログイン情報が満足するか否かを判定し、
上記条件が満足されるとき、上記ユーザは、上記要求した共有ファイルにアクセスする権利があると判定することを特徴とするアクセス権利判定プログラム。
【請求項２０】　請求項１９記載のアクセス権利判定プログラムを格納した記憶媒体において、
上記コンピュータは、上記クライアント情報処理装置にログオンし得る各ユーザーのについての予め定められた属性情報が記述されたユーザー情報ファイルが予め格納されており、
上記ログイン情報は、上記クライアント情報処理装置における上記ユーザーに関するＣｏｏｋｉｅデータであり、
上記開示先リストは、個人に関する予め定められた属性情報が記述され、
上記アクセス権利判定プログラムは、上記Ｃｏｏｋｉｅデータが示すユーザーに関する属性を、上記ユーザーファイルから検出し、
上記検出した属性が、上記開示先リストが示す条件を満足するか否かを判定することを特徴とするアクセス権利判定プログラムを格納した記憶媒体。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、共有ファイルを通信回線を介して送受信するための、共有ファイル送受信システムに係り、特に、アクセス制御機能を備える共有ファイル送受信システムに関する。
【０００２】
【従来の技術】インターネットと呼ばれる世界的規模のネットワークの普及と共に、このインターネットと企業内ネットワークを接続し、インターネットを介して情報を送受信するケースが増大している。また、前記インターネットにおいては、情報発信機能を持つWWW（Ｗｏｒｌｄ－Ｗｉｄｅ　Ｗｅｂ）サーバを利用し、ハイパーテキストと呼ばれる形式の文書ファイルで情報を提供することが一般的となっている。前記ハイパーテキストを解釈し、グラフィカルに表示するソフトウェアはブラウザと呼ばれ、広く普及している。前記ハイパーテキストの言語仕様としては、ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）が一般に用いられている。この言語仕様について、および、ＨＴＭＬで記述されたファイルを表示するためのブラウザについては、例えば、「ＵＮＩＸ　ＭＡＧＡＺＩＮＥ」（ＡＳＣＩＩ社、１９９４．１０）ｐｐ．５２－６０に記載されている。なお、殆どのＨＴＭＬファイルは、他のＨＴＭＬファイルやイメージデータファイルとリンクしており、前記ブラウザは、ＨＴＭＬファイルを受信した後で、それがリンクしているイメージデータファイルを受信し、該ＨＴＭＬファイルの内容と合わせて同一画面に表示する。これらＨＴＭＬファイルとそれにリンクされたイメージデータファイルを総括してページと呼ぶ。
【０００３】上記WWWサーバの多くは、機密情報を含むページを格納するためのアクセス制御機能として、特定の端末に対するページの送信を許可、または拒否する機能や、ユーザーが正しいパスワードを入力することによってページの送信を許可する機能を備えている。これらの機能については、「ＯＰＥＮ　ＤＥＳＩＧＮ」（ＣＱ出版社、１９９７．１０）ｐｐ．１１４－１２５などに記載されている。
【０００４】
【発明が解決しようとする課題】しかし、上述のWWWサーバが持っているアクセス制御機能を利用する場合、WWWサーバに対してアクセス権利の設定を行うことができる者は、WWWサーバの特権ユーザーに限られるという問題がある。
【０００５】また、アクセス制御に関する情報が各々のWWWサーバに分散してしまうため、アクセス制御に関する情報を変更する際の手間が大きいという問題がある。

【０００６】そして、アクセス制御の設定方法は、ＷＷＷサーバ毎に定められているため、個々のＷＷＷサーバ毎にアクセス制御の設定方法を覚えなければならないという問題がある。

【０００７】さらに、複数のＷＷＷサーバに跨って情報が保存されている場合には利用者が情報を閲覧するために個々のＷＷＷサーバにログインしなければならないという問題がある。

【０００８】本発明の第１の目的は、情報作成者がアクセス権利を容易に設定できるようなアクセス制御機能を備えた共有ファイル送受信システムを提供することにある。

【０００９】本発明の第２の目的は、アクセス制御に関する情報の変更が容易に行えるアクセス制御機能を備える共有ファイル送受信システムを提供することにある。

【００１０】本発明の第３の目的は、情報が複数のＷＷＷサーバに跨っている場合でも、システム全体として一度ログインするだけで、アクセスする権利を持っている、すべてのページにアクセス可能なアクセス制御機能を備える共有ファイル送受信システムを提供することにある。

【００１１】本発明の第４の目的は、さまざまなＷＷＷサーバが利用されている環境においても、システム全体としては同一の方法で設定可能なアクセス制御機能を備える共有ファイル送受信システムを提供することにある。

【００１２】

【課題を解決するための手段】上記目的を達成するため、本発明の第１の態様によれば、通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、共有ファイルにアクセスする権利をデータ受信側の利用者が有するか否かを判定するためのアクセス権利判定手段と、データ送信側の端末からデータ受信側の端末にファイルを転送するためのデータ中継手段とを備え、前記共有ファイルは、アクセス権利を持つ利用者を示す開示先情報が予め付加され、前記アクセス権利判定手段は、共有ファイルにアクセスする権利をデータ受信側の利用者が持つか否かを、当該共有ファイルに付加されている前記開示先情報に基づいて判定し、前記データ中継手段は、前記データ受信側の利用者の要求に応じてデータ送信側の端末から共有ファイルを受信し、当該受信した共有ファイルに対するアクセス権利を前記利用者が有すると前記アクセス権利判定手段が判定した場合にのみ、前記受信した共有ファイルをデータ受信側の端末に送信することを特徴とする共有ファイル送受信システムが提供される。

【００１３】本発明の第２の態様によれば、通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、アクセスする権利を判定するためのアクセス権利判定装置と、データ受信側の前記端末に前記データを送信するデータ中継装置とが通信回線を介して接続され、前記アクセス権利判定装置は、前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わせられて記述されたリストを基に、データ受信側の前記端末の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定し、前記データ中継装置は、データ送信側の端末から前記共有ファイルを受信し、当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、前記利用者に当該共有ファイルに対するアクセス権利があると前記アクセス権利判定装置が判定した場合にのみ、データ受信側の前記端末に前記データを送信することを特徴とする共有ファイル送受信システムが提供される。

【００１４】本発明の第３の態様によれば、共有ファイルを格納するための機能、および、転送要求を受けた共有ファイルを転送するための機能を有するサーバ装置と、前記サーバ装置から共有ファイルを受信するための機能、および、ユーザーに共有ファイルの情報を表示するための機能を有するクライアント装置と、共有ファイルの転送要求を前記クライアント装置から前記サーバ装置に中継し、共有ファイルを前記サーバ装置から前記クライアント装置に中継するための機能、および、当該共有ファイルをキャッシュするためのキャッシュ機能を有する代理サーバ装置と、前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わせられた記述されたリストを基に、前記クライアント装置の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定するためのアクセス権利判定装置と、前記サーバ装置から前記共有ファイルを受信し、当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、前記アクセス権利判定装置が前記利用者に当該共有ファイルに対するアクセス権利があると判定した場合にのみ、前記代理サーバ装置に前記データを送信するデータ中継装置とが通信回線を介して接続されていることを特徴とする共有ファイル送受信システムが提供される。

【００１５】本発明の第４の態様によれば、通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、通信回線を介して受信する前記情報は、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストであって、アクセス権利を持つか否かの判断を依頼した依頼者を特定するための依頼者認証手段と、当該アクセス権利判定装置が管理する前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するためのアクセス権利判定手段とを備えることを特徴とするアクセス権利判定装置が提供される。

【００１６】本発明の第５の態様によれば、通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、通信回線を介して受信する情報とは、前記依頼者の属性情報を、暗号鍵と呼ばれる情報によって暗号化したものと、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストとであって、当該アクセス権利判定装置は、前記暗号化された属性情報を、前記依頼者が当該アクセス権利判定装置に登録した、復号鍵と呼ばれる情報によって復号する属性情報復号手段を備え、前記アクセス権利判定手段は、前記属性情報復号手段によって復号化した、前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するものであることを特徴とするアクセス権利判定装置が提供される。

【００１７】本発明の第６の態様によれば、共有ファイルに対するアクセス権利を持つか否かをコンピュータを用いて判定するためのアクセス権利判定プログラムを格納した記憶媒体において、共有ファイルを要求しているユーザーが、ログインしているクライアント情報情報処理装置から、当該ユーザーのログイン情報を取得し、上記ユーザーが要求している共有ファイルを、サーバー情報処理装置から取得し、上記取得した共有ファイルに付加されている開示先リストに示されている条件を、上記取得したログイン情報が満足するか否かを判定し、上記条件が満足されるとき、上記ユーザは、上記要求した共有ファイルにアクセスする権利があると判定することを特徴とするアクセス権利判定プログラムを格納した記憶媒体が提供される。

【００１８】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態について説明する。

【００１９】まず、図１を参照して、本発明がＷＷＷ（Ｗｏｒｌｄ－Ｗｉｄｅ　Ｗｅｂ）システムに適用されたファイル共有システムの構成の概略について説明する。

【００２０】図１において、本実施の形態におけるファイル共有システム１０は、ＷＷＷのサーバ機能を備えるサーバ情報処理装置１１と、ＷＷＷのクライアント機能を備えるクライアント情報処理装置１２と、前記サーバ情報処理装置１１およびクライアント情報処理装置１２で送受されるデータを中継する機能を備えるデータ中継処理装置１３と、前記中継しようとするデータのアクセス権利を判定するためのアクセス権利判定処理装置１４とが、ネットワーク１に接続されて構成されている。

【００２１】上記ネットワーク１としては、例えば、企業内のネットワークなどのローカルエリアネットワーク（ＬＡＮ）が適用され、前記各処理装置が、ＬＡＮケーブル１５を介して相互に接続されて構成される。

【００２２】前記アクセス権利判定処理装置１４は、前記サーバ情報処理装置１１から前記クライアント情報処理装置１２に送信されるデータに対して、前記クライアント情報処理装置１２にログインしている利用者（ログインユーザー）（以下、単に、利用者、ユーザーとも称する）が当該データにアクセスする権利を持つかどうかを判定する機能を備える。

【００２３】ここで、図１では、ネットワーク１に一つのクライアント情報処理装置１２が接続されている場合を示しているが、接続されるクライアント情報処理装置１２の数はこれに限らず、クライアント情報処理装置１２がＬＡＮケーブル１５に複数接続されてもよいことは勿論である。

【００２４】また、図１では、ネットワーク１に一つのサーバ情報処理装置１１が接続されている場合を示しているが、接続されるサーバ情報処理装置１１の数はこれに限らず、サーバ情報処理装置１１がＬＡＮケーブル１５に複数接続されてもよいことは勿論である。

【００２５】同様に、複数のデータ中継処理装置１３がＬＡＮケーブル１５に接続されていてもよい。また、複数のアクセス権利判定処理装置１４がＬＡＮケーブル１５に接続されていてもよい。

【００２６】なお、前記各処理装置は、ＬＡＮケーブル１５に代えて、電話回線などを介して前記ネットワーク１に接続されてもよい。例えば、前記クライアント情報処理装置１２と前記データ中継処理装置１３とが互いに離れた場所に存在する場合、ＬＡＮケーブル１５に代えて、電話回線などで両者を接続することができる。また、各処理装置相互のデータ転送トラフィックに応じて、より転送容量、速度が大きな伝送路で、特定の処理装置同士を接続することができる。

【００２７】前記サーバ情報処理装置１１は、中央処理装置（ＣＰＵ）１１１と、メモリ１１２と、ＬＡＮコントローラ１１３と、ディスクコントローラ１１４と、磁気ディスク１１５とを備えて構成される。

【００２８】サーバ情報処理装置は、起動時に、磁気ディスク１１５に格納されているオペレーティングシステム（ＯＳ）１１５ａおよびＷＷＷサーバプログラム１１５ｂを、ディスクコントローラ１１４を介して、メモリ１１２上にロードする。そして、ＣＰＵ１１１がＷＷＷサーバプログラム１１５ｂを実行することで、ＷＷＷサーバとして機能する。

【００２９】すなわち、サーバ情報処理装置１１は、磁気ディスク１１５にＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）ファイルや画像ファイルを格納したり、クライアント情報処理装置１２がデータ中継処理装置１３を介して要求した、ＨＴＭＬファイル、または、これに加えて、当該ＨＴＭＬファイル２００にリンク（参照指定）された画像ファイル、動画ファイル、音声ファイルなど（以下、被参照ファイルともいう）を、前記クライアント情報処理装置１２に転送す

る。

【００３０】WWWサーバプログラム１１５ｂとしては、WWWシステムに用いられる既存のプログラムを変更することなく、そのまま使用することができる。

【００３１】なお、WWWサーバプログラム１１５ｂは、当該WWWサーバプログラム１１５ｂが備えるアクセス制御機能を利用して、データ中継処理装置１３からのアクセスのみを受け付けるように設定されている。

【００３２】前記クライアント情報処理装置１２は、ＣＰＵ１２１と、メモリ１２２と、ＬＡＮコントローラ１２３と、ディスクコントローラ１２４と、磁気ディスク１２５とを備えて構成される。

【００３３】クライアント情報処理装置１２は、起動時に、磁気ディスク１２５に格納されているＯＳ１２５ａを、ディスクコントローラ１２４を介して、メモリ１２２にロードする。

【００３４】また、クライアント情報処理装置１２は、ユーザーの指示に従い、ブラウザプログラム１２５ｂを、ディスクコントローラ１２４を介して、磁気ディスク１２５からメモリ１２２上にロードする。そして、ＣＰＵ１２１がブラウザプログラム１２５ｂを実行することで、WWWクライアントの機能を実現している。すなわち、クライアント情報処理装置１２は、WWWクライアントとして、ユーザーが要求するＨＴＭＬファイルや被参照ファイルなどの転送を前記サーバ情報処理装置１１に要求し、また、前記サーバ情報処理装置１１から転送されてきたＨＴＭＬファイル、または、これに加えて画像ファイルなどの被参照ファイルを表示する。

【００３５】なお、ブラウザプログラム１２５ｂは、プロキシサーバ（代理サーバ）を設定する機能を利用して、前記サーバ情報処理装置１１とデータの送受を行う際には、必ず前記データ中継装置１３を介して行うように設定されている。

【００３６】ブラウザプログラム１２５ｂとしては、プロキシサーバを利用できるものであれば、WWWシステムに用いられる既存のプログラムを変更することなく、そのまま使用することができる。

【００３７】また、クライアント情報処理装置１２は、ユーザーの指示に従い、アクセス権利設定プログラム１２５ｃを、ディスクコントローラ１２４を介して、磁気ディスク１２５からメモリ１２２にロードする。

【００３８】アクセス権利設定プログラム１２５ｃは、ＨＴＭＬファイルに対して、アクセス権利を設定するためのものである。ＨＴＭＬファイルとしては、ユーザーが作成するなどして、予め磁気ディスク１２５に格納されているものを想定して説明するが、アクセス権利の設定を行いつつ、作成するものであってもよい。

【００３９】前記データ中継処理装置１３は、ＣＰＵ１３１と、メモリ１３２と、ＬＡＮコントローラ１３３と、ディスクコントローラ１３４と、磁気ディスク１３５とを備えて構成される。

【００４０】データ中継処理装置１３は、起動時に磁気ディスク１３５に格納されているＯＳ１３５ａと、データ中継処理プログラム１３５ｂとをディスクコントローラ１３４を介して、メモリ１３２にロードする。データ中継処理プログラム１３５ｂは、前記クライアント情報処理装置１２から送信されてきた、ＨＴＭＬファイルや被参照ファイルなどの転送要求を前記サーバ情報処理装置１１に送信したり、前記サーバ情報処理装置１１から送信されてきたＨＴＭＬファイルや画像ファイルに対して、ユーザーがアクセスする権利を持つかどうかを前記アクセス権利判定装置１４に確認し、アクセスする権利を持つ場合には当該ＨＴＭＬファイルや画像ファイルを前記クライアント情報処理装置１２に送信するためのものである。

【００４１】前記アクセス権利判定装置１４は、ＣＰＵ１４１と、メモリ１４２と、ＬＡＮコントローラ１４３と、ディスクコントローラ１４４と、磁気ディスク１４５とを備えて構成される。

【００４２】アクセス権利判定装置１４は、起動時に、磁気ディスク１４５に格納されているＯＳ１４５ａと、アクセス権利判定プログラム１４５ｂとをディスクコントローラ１４４を介して、メモリ１４２にロードする。

【００４３】なお、アクセス権利判定装置１４は、パスワード管理ファイル１４５ｃと、ユーザーＩＤ情報ファイル１４５ｄと、共有グループ定義ファイル１４５ｅとを磁気ディスク１４５に格納している。

【００４４】アクセス権利判定プログラム１４５ｂは、ユーザーのパスワード情報をパスワード管理ファイル１４５ｃによって管理する。前記パスワード情報は、前記アクセス権利判定プログラム１４５ｂの指示によって前記メモリ１４２にロードされ、ユーザーを特定するために用いられる。

【００４５】また、アクセス権利判定プログラム１４５ｂは、ユーザーＩＤ情報ファイル１４５ｄによって予め定義されているユーザーの個人情報、および、共有グループ定義ファイル１４５ｅによって予め定義されている共有グループ情報を管理する。前記ユーザーＩＤ情報および前記共有グループ定義情報は、前記アクセス権利判定プログラム１４５ｂの指示によって前記メモリ１４２にロードされ、アクセスする権利を持つか否かを判定するために用いられる。

【００４６】以下、上述したファイル共有システム１０の主な構成について、詳細に説明する。

【００４７】まず、図２を参照して、前記ユーザーＩＤ情報ファイル１４５ｄについて説明する。

【００４８】ユーザーＩＤ情報ファイル１４５ｄでは、個人に関する属性のカテゴリを示す情報と、属性の内容を示す情報とが互いに対応付けられ、情報の組として記述される。ユーザーＩＤ情報ファイル１４５ｄによって

記述される属性のカテゴリの数は、１つであっても、複数であってもよい。複数のカテゴリについて、属性を記述する場合、１つのカテゴリについて属性を記述する情報の組を、複数組記述することが好適である。

【００４９】図２に示されるユーザーＩＤ情報ファイル１４５ｄは、１０組の情報の組が記述され、１０のカテゴリについて、属性を登録している。そして、カテゴリを示す情報として、カテゴリを識別するためのカテゴリ番号が用いられている。また、いくつかのカテゴリについて、そのカテゴリの属性の内容を示す情報として、予め定められたコードが用いられている。

【００５０】なお、本実施の形態では、ユーザーＩＤ情報ファイル１４５ｄに登録され得るカテゴリは予め定められ、これらのカテゴリを予め定められた順序で、欠番および重複なくなく並べる形式としている。すなわち、属性の内容を示す情報が、予め定められた順番で並べられ、その情報が現れる順番によりカテゴリを示している。このため、アクセス権利判定装置１４（図１参照）の前記磁気ディスク１４５（図１参照）に実際に記憶されるのは、属性の内容を示すデータだけ、あるいは、データに加えてコードの値とすることができる。

【００５１】次に、図３を参照して、前記共有グループ情報ファイル１４５ｅ（図２参照）について説明する。

【００５２】図３において、共有グループ情報ファイル１４５ｅは、共有グループ情報と、当該共有グループ情報の名称と、当該共有グループの作成者の識別子と、作成日時とが互いに対応付けられた情報組が、１組または複数組登録される。図３に示される例では、６組の情報組が登録されている。

【００５３】前記共有グループ情報１４５ｅにおいては、アクセスを許可する条件がリスト形式で記述されている。以下、このリストを開示先リストを呼ぶ。

【００５４】開示先リストは、アクセスを許可すべきユーザーの条件（以下、追加条件という）、または、アクセスを拒否すべきユーザーの条件（以下、除外条件という）が記述される項を少なくとも１つ含む。項は、その項が追加条件を示すか、除外条件を示すかを示す区切り記号に続けて記述され、複数の項が含まれる場合、区切り記号により区切られて並べられる。前記追加条件を示す区切り記号としては、カンマ（，）が用いられ、前記除外条件を示す区切り記号としては、マイナス（－）が用いられる。ただし、追加条件を示す項が、開示先リストの先頭に現れる場合には、その項の区切り記号（，）は省略される。

【００５５】前記項は、ユーザーの条件が関係演算子で記述された条件式を少なくとも１つ含む。条件式は、ユーザーの条件を、ユーザーＩＤ情報ファイル１４５ｄにおける属性、または、他のグループを示すグループ名称を指定するためのものである。共通する項に、複数の条件式が含まれる場合、条件式と条件式とは、論理演算子（＾）で連結される。この論理演算子（＾）は、論理積の意味を持つ。

【００５６】各条件式は、「カテゴリ番号」と、「グループ／データ／コード識別子」と、「関係演算子」と、「条件データ」とが互いに対応付けられて記述されている。

【００５７】前記「カテゴリ番号」は、条件の指定に用いるデータのカテゴリを示すためのものである。

【００５８】前記「グループ／データ／コード識別子」は、前記カテゴリ番号により示されるカテゴリにおけるデータの種類を識別するためのものである。グループ／データ／コード識別子としては、条件の指定に用いられるデータの種類が、他の開示先リストにより定義されたグループ名称で記述されることを示すＧ（Ｇｒｏｕｐ）と、ユーザーＩＤ情報ファイル１４５ｄにおけるデータの情報を用いることを示すＤ（Ｄａｔａ）と、ユーザーＩＤ情報ファイル１４５ｄにおけるコードの情報を用いることを示すＣ（Ｃｏｄｅ）とを用いることができる。

【００５９】前記「条件データ」は、関係演算子と共に、条件を指定するためのものであり、前記「カテゴリ番号」および「グループ／データ／コード識別子」で指定された情報に対応して、「条件データ」としては、グループ名称、データ、コードのいずれかが用いられる。前記関係演算子、としては、等しい（＝）、等しくない（≠）、大きい（＞）、小さい（＜）を用いることができる。なお、前記「条件データ」が数値以外の文字列である場合、文字コードの数値を用いて、関係演算子が指定する関係を定義することができるここで、前記関係演算子の演算は、前記論理演算子および区切り記号の演算に先行して演算され、また、前記論理演算子の演算は、区切り記号の演算に先行して演算される。なお、区切り記号の演算は、左から右に順番に演算される。

【００６０】例えば、図２で示した前記ユーザーＩＤ情報１４５ｄの定義と、図３で示した前記共有グループ情報１４５ｅとを用いた場合、「本社の資材グループと、システム研究所の第四部の主任以上と、暗号太郎」という開示先に対する共有グループ情報は、「０Ｇ＝本社資材，５Ｃ＝６７６＾６Ｃ＝０４＾８Ｃ＞＝５，２Ｄ＝暗号太郎」という開示先リストになる。すなわち、この開示先リストは、追加条件を示す項３つで記述され、このうち、第２項は、３つの条件式の論理積で記述されている。

【００６１】また、「本社のうちの営業以外と、システム研究所のうちの安全課以外とであって、かつ、氏名コード6781901001および678951010を除く」という開示先に対する共有グループ情報は、「５Ｃ＝００１＾６Ｃ≠２１，５Ｃ＝６７６＾７Ｃ≠４０２－４Ｃ＝6781901001－４Ｃ＝678951010」という開示先リストになる。すなわち、この開示先リストは、追加条件を示す項２つと、除外条件を示す項２つとで記述され、このうち、第１項

および第２項は、それぞれ２つの条件式の論理式で記述されている。

【００６２】次に、図４を参照して、アクセス権利をＨＴＭＬファイルに対して設定する方法、および、アクセス権利が設定されたＨＴＭＬファイルについて説明する。

【００６３】図４（ａ）において、ＨＴＭＬファイル３００は、サーバー情報処理装置１１（図１参照）のユーザー（以下、ＨＴＭＬファイルのオーナー、または、単にオーナーともいう）が作成したＨＴＭＬファイルの例である。ユーザーは、テキストエディタやＨＴＭＬエディタなどを用いて、図４（ａ）に示すようなＨＴＭＬファイルを作成することができる。

【００６４】ここで、ＨＴＭＬファイルのオーナーとは、当該ＨＴＭＬファイルにアクセスする権利を設定する権利を持つ者を指し、当該ＨＴＭＬファイルを作成した者だけでなく、このファイルを改変する権利を持つ者、および、アクセス権利を設定、変更する権利のみを有する者を含み、一人のユーザーである場合だけでなく、複数人のユーザが属するグループなどであってもよい。

【００６５】なお、上記アクセス権利を設定、変更する権利のみを有する者とは、例えば、サーバー情報処理装置１１（図１参照）において、ＨＴＭＬファイルを書き換える権利はないが、アクセス権利設定プログラム１２５ｃを実行する権利は有する者として設定することができる。

【００６６】次に、ＨＴＭＬファイルのオーナーは、前記アクセス権利設定プログラム１２５ｃによって、ＨＴＭＬファイルにアクセス権利を設定する。

【００６７】図４（ｂ）において、ＨＴＭＬファイル４００は、図４（ａ）に示されるＨＴＭＬファイル３００に、アクセス権利が設定されたＨＴＭＬファイルの例である。

【００６８】アクセス権利が設定されたＨＴＭＬファイル４００は、アクセス権利が設定される前のＨＴＭＬファイル４２０の先頭部分に、アクセス制御のためのヘッダ４１０（以降、当該ヘッダをアクセス制御ヘッダと呼ぶ）４１０を付加したものになっている。

【００６９】図４（ｃ）を参照して、ＨＴＭＬファイル４００（図４（ｂ）参照）における、アクセス制御ヘッダ４１０（図４（ｂ）参照）の詳細について説明する。

【００７０】図４（ｃ）において、前記アクセス制御ヘッダ４１０は、アクセス制御ヘッダであることを示す文字列を記述するための領域４１１と、当該ＨＴＭＬファイルにアクセス権利を設定したオーナーの識別子を記述するための領域４１２と、当該ＨＴＭＬファイルにアクセス権利を設定した日付を記述するための領域４１３と、当該ＨＴＭＬファイルにアクセスを許可するユーザー条件の開示先リストを記述するための領域４１４と、当該ＨＴＭＬファイルにアクセスする権利がない場合に表示すべきメッセージが格納されたメッセージファイルを示すリンク情報（参照先を指定する情報）を記述するための領域４１５と、当該ＨＴＭＬファイルのアクセス権利を判定するアクセス権利判定装置１４（図１参照）のホスト名を記述するための領域４１６とを含んで構成される。

【００７１】前記領域４１５に記録されている、アクセスする権利がない場合に表示するメッセージファイルのリンク情報は、例えば、ＷＷＷシステムに適用される場合、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒｓ）形式で記述することが便利である。アクセスする権利がない場合に表示すべきメッセージを記録したファイルは、前記サーバ情報処理装置１１（図１参照）の磁気ディスク１１５（図１参照）に格納されている。なお、メッセージファイルのリンク情報に代えて、メッセージそのものを格納してもよい。また、当該ＨＴＭＬファイルにアクセスする権利がない場合であっても、メッセージを表示せず、ユーザー透過的な情報提示態様とすることも可能である。この場合、メッセージ、または、それを格納したメッセージファイルを、前記領域４１５に格納することは省略される。

【００７２】ここで、前記アクセス制御ヘッダ部分４１０は、ＨＴＭＬにおけるコメントを記述する文法を利用して記述されている。このため、当該ＨＴＭＬファイルをブラウザプログラムで直接表示した場合でも、余分な情報が表示されることや、画面が乱れること、を防ぐことができる。

【００７３】アクセス権利が設定されたＨＴＭＬファイル４００は、通常のＨＴＭＬファイルと同様に、前記サーバ情報処理装置１１（図１参照）の磁気ディスク１１５（図１参照）に格納される。

【００７４】次に、図５、６、および、図９から１２を参照して、アクセス権利設定プログラム１２５ｃについて説明する。

【００７５】まず、図６を参照して、アクセス権利設定プログラム１２５ｃのモジュール構成について説明する。

【００７６】図６において、アクセス権利設定プログラム１２５ｃは、ログイン処理ルーチン１１００と、アクセス権利設定ルーチン１２００と、ログアウト処理ルーチン１３００とを含んで構成される。

【００７７】次に、図５を参照して、アクセス権利設定プログラム１２５ｃの動作フローについて説明する。

【００７８】図５において、アクセス権利設定プログラム１２５ｃは、まず、ステップ１００１で、前記ログイン処理ルーチン１１００を実行し、アクセス権利を設定しようとしているユーザーを特定するための処理を行う。ログイン処理ルーチン１１００は、アクセス権利を設定しようとしているユーザーを特定するため（すなわ

ち、当該ＨＴＭＬファイルのオーナーであるか否かを判定するため）に、アクセス権利判定プログラム１４５ｂに対してログイン処理を行うためのものである。ログイン処理ルーチン１１００におけるログイン処理では、前記アクセス権利判定プログラム１４５ｂに何度もログインすることを防止するため、ログイン証明書を用いる。ログイン証明書は、アクセスしているユーザーが、過去に前記アクセス権利判定プログラム１４５ｂにログインした正当なユーザーであることを保証するものである。ログイン処理ルーチン１１００における処理の詳細については後述する。

【００７９】次に、ユーザーの特定が成功したか否かを判定する(ステップ１００２)。ユーザーの特定に成功したと判定された場合には、ステップ１００３に移行し、イベント待ち状態をとる。イベントが到着すると、イベントがアクセス権利設定要求か否かを調べる（ステップ１００４）。

【００８０】アクセス権利設定要求である場合には、ステップ１００８に移行し、前記アクセス権利設定ルーチン１２００を実行して、ステップ１００３に戻る。一方、アクセス権利設定要求でない場合には、ステップ１００５に移行し、イベントがログアウト要求か否かを調べる。

【００８１】ログアウト要求であれば、前記ログアウト処理ルーチン１３００を実行し、ログアウト処理を行う。ステップ１００７で、ログアウトに成功すると、プログラムを終了する。一方、ログアウトに失敗した場合には、ステップ１００３に戻る。

【００８２】図９を参照して、ログイン証明書の構成について説明する。

【００８３】図９において、ログイン証明書２００は、ログイン証明書の識別番号を記述するための領域２０１と、前記ユーザーの識別子を記述するための領域２０２と、ログイン証明書の発行日時を記録するための領域２０３と、当該ログイン証明書を使用してアクセスを行った回数を記述するための領域２０４と、当該ログイン証明書を使用して最後にアクセスを行った日時を記録するための領域２０５とを含んで構成されている。

【００８４】なお、本実施の形態におけるログイン証明書の形式は、Ｃｏｏｋｉｅと呼ばれる形式を利用している。Ｃｏｏｋｉｅは、ブラウザの状態を保存するために一般的に用いられている形式である。前記ブラウザプログラム１２５ｂがログイン証明書を保持することが、Ｃｏｏｋｉｅの形式を利用することにより可能となる。従って、後述するＨＴＭＬファイルを閲覧する際に、前記ブラウザプログラム１２５ｂが、前記クライアント情報処理装置１２の利用者を特定することができる。

【００８５】図１０を参照して、アクセス権利設定プログラムにおける前記ログインルーチン１１００の動作フローについて説明する。

【００８６】まず、ログイン証明書を持っているかどうかを調べる（ステップ１１０１）。ログイン証明書を持っている場合には、ログイン証明書が有効であるかどうかを調べるためにログイン証明書を前記アクセス権利判定プログラム１４５ｂに送信する（ステップ１１０２）。

【００８７】次に、送信したログイン証明書が有効かどうかの判定結果を受信する（ステップ１１０３）。ログイン証明書が有効であった場合には、ステップ１００７以下を実行して、新しいログイン証明書の発行と、古いログイン証明書の破棄を行い、処理を終了する。

【００８８】一方、ログイン証明書が有効でなかった場合には、ＩＤとパスワードとをユーザーから取得する（ステップ１１０４）。次に、ユーザー認証処理を行う（ステップ１１０５）。ユーザー認証処理においてログインに成功した場合には、新しいログイン証明書の発行（ステップ１１０７）と、古いログイン証明書の破棄（ステップ１１０８）とを行い、処理を終了する。

【００８９】ステップ１１０５におけるユーザー認証処理でログインに失敗した場合には、ステップ１１０９に移行し、３回続けて失敗するまでは、ステップ１１０４～ステップ１１０６の処理を繰り返すように制御する。３回続けて失敗した場合には、ステップ１１０８を実行する。

【００９０】なお、本実施の形態では、ログイン証明書が有効かどうかを確認するための処理をアクセス権利判定プログラム１４５ｂで行っているが、この処理を、ログイン処理ルーチンに処理１１００を組み込んでもよい。

【００９１】図１１を参照して、アクセス権利設定プログラム１２５ｃの前記ログアウト処理ルーチン１３００の動作フローについて説明する。ログアウト処理ルーチン１３００は、アクセス権利判定プログラム１４５ｂ（図６参照）に対してログアウト処理を行うためのものである。

【００９２】図１１において、まず、ステップ１３０１で、現在オープン中のファイルがあるかどうかを調べる。オープン中のファイルがない場合には、ステップ１３０４以下を実行し、アクセス権利判定プログラム１４５ｂからのログアウト処理を行う。オープン中のファイルがある場合には、ログアウト処理を中断するかどうかをユーザーに確認する（ステップ１３０２）。ログアウト処理を中断する場合には、処理を終了する。ログアウト処理を続行する場合には、ステップ１３０３で、オープン中のファイルをクローズする。次に、ステップ１３０４で、前記アクセス権利判定プログラム１４５ｂにログイン証明書を送信し、ログイン証明書を無効化する。

【００９３】図１２を参照して、アクセス権利設定プログラムの前記アクセス権利設定ルーチン１２００の動作フローについて説明する。アクセス権利設定ルーチン１

２００は、ユーザーが作成したＨＴＭＬファイルにアクセス権利を設定するためのものである。すなわち、サーバ情報処理装置１１（図１参照）のユーザーが、当該ユーザーがオーナーであるＨＴＭＬファイルのアクセス権利を設定するために用いられる。

【００９４】まず、ステップ１２０１で結果を一時的に出力する一時ファイルを作成する。次に、ステップ１２０２で前記開示先リストを作成する。ステップ１２０３では、作成した開示先リストを含めたヘッダ部分を一時ファイルに書き込む。次に、ステップ１２０４でアクセス権利を設定するＨＴＭＬファイル（以降、入力ファイルと呼ぶ）のデータをバッファに読み込む。次に、ステップ１２０５で入力ファイルから、すべてのデータを読み込み終えたかどうかを調べる。これは、読み込んだデータのサイズが０であれば、入力ファイルから、すべてのデータを読み込み終えたと判断する。入力ファイルから、すべてのデータを読み込み終えていない場合には、ステップ１２０６で一時ファイルに読み込んだデータを書き込み、ステップ１２０４に戻る。一方、入力ファイルのすべてのデータを読み込み終えている場合には、入力ファイルをクローズし（ステップ１２０７）、一時ファイルもクローズする（ステップ１２０８）。次に、ステップ１２０９で、アクセス権利を設定したＨＴＭＬファイル（以降、出力ファイルと呼ぶ）のファイル名が入力ファイルのファイル名と一致しているかどうかを調べる。ファイル名が一致していない場合には、一時ファイルのファイル名を出力名に変更し、処理を終了する。一方、ファイル名が一致している場合には、ステップ１２１０で入力ファイルを削除した後、一時ファイルのファイル名を出力ファイル名に変更し、処理を終了する。

【００９５】図１３を参照して、ユーザーが、アクセス権利が設定されたＨＴＭＬファイルを閲覧する場合の動作の概略について説明する。図１３には、アクセス権利が設定されたＨＴＭＬファイルを、前記サーバ情報処理装置１１と前記クライアント情報処理装置１２との間で送受する場合に、本実施の形態における各プログラム間で送受されるデータのフローが描かれている。

【００９６】図１３において、まず、ユーザーは、前記ブラウザプログラム１２５ｂにＨＴＭＬファイルを要求する。

【００９７】次に、前記ブラウザプログラム１２５ｂは、前記データ中継プログラム１３５ｂに前記要求を転送する。転送に際し、前記ブラウザプログラム１２５ｂが前記ログイン証明書を保持している場合には、当該ログイン証明書も同時に転送する。前記データ中継プログラム１３５ｂは、前記ＷＷＷサーバプログラム１１５ｂに前記要求を転送し、前記ＷＷＷサーバプログラム１１５ｂから要求したＨＴＭＬファイルを受信する。ＨＴＭＬファイルを受信した、前記データ中継プログラム１３５ｂは、前記アクセス権利判定プログラム１４５ｂに対して、ログイン証明書を転送し、ユーザー認証処理を行う。

【００９８】次に、前記データ中継プログラム１３５ｂは、ＨＴＭＬファイルから開示先リストを取り出し、前記アクセス権利判定プログラム１４５ｂに転送する。前記アクセス権利判定プログラム１４５ｂは、開示先リストの条件にユーザーのＩＤ情報が適合するかどうかを調べ、結果を前記データ中継プログラム１３５ｂに通知する。前記結果を受信した前記データ中継プログラム１３５ｂは、前記アクセス権利判定プログラム１４５ｂが「ユーザーは当該ＨＴＭＬファイルに対しアクセス権利を持つ」と判定した場合には、当該ＨＴＭＬファイルを前記ブラウザプログラム１２５ｂに転送する。一方、前記アクセス権利判定プログラム１４５ｂが「ユーザーは当該ＨＴＭＬファイルに対してアクセス権利を持たない」と判定した場合には、当該ＨＴＭＬファイルからエラーメッセージファイルのファイル名を取り出し、前記ＷＷＷサーバプログラム１１５ｂにエラーメッセージファイルを要求する。そして、前記ＷＷＷサーバプログラム１１５ｂから受信したエラーメッセージファイルを前記ブラウザプログラム１２５ｂに転送する。最後に、前記ブラウザプログラム１２５ｂは、前記データ中継プログラム１３５ｂから受信した、ファイルを前記クライアント情報処理装置１２の画面に表示する。

【００９９】次に、図２０から図２２を参照して、ＨＴＭＬファイルの転送を要求した場合に表示される画面について説明する。

【０１００】図２０は、図４（ｂ）の前記ＨＴＭＬファイルに対してアクセスする権利を持つユーザーが、図４（ｂ）の前記ＨＴＭＬファイルの転送を要求した場合に表示される画面の例である。

【０１０１】一方、図２１は、図４（ｂ）の前記ＨＴＭＬファイルに対してアクセスする権利を持たないユーザーが、図４（ｂ）の前記ＨＴＭＬファイルの転送を要求した場合に表示される画面の例である。なお、この例では、前記サーバー情報処理装置１１には、エラーメッセージファイルとして、図２２のファイルが格納されている。

【０１０２】次に、図８、１４、１５を参照して、前記データ中継処理プログラム１３５ｂについて説明する。

【０１０３】まず、図８を参照して、前記データ中継処理プログラム１３５ｂのモジュール構成について説明する。

【０１０４】前記データ中継処理プログラム１３５ｂは、ログイン処理ルーチン２０００と、ログアウト処理ルーチン２１００と、データ中継処理ルーチン２２００と、アクセス権利確認ルーチン２３００とを含んで構成される。

【０１０５】前記データ中継処理ルーチン２２００は、サーバ情報処理装置１１とクライアント情報処理装置１

２との間で行われる、データの送受を中継するためのものである。

【０１０６】次に、図１４を参照して、データ中継処理ルーチン２２００の動作フローについて説明する。

【０１０７】まず、ステップ２２０１で、前記ブラウザプログラム１２５ｂからの要求を待ち受ける。要求がくると、ステップ２２０２で、要求にログイン証明書が含まれているかどうかを調べる。ログイン証明書が含まれていない場合には、ステップ２２０４以下を実行する。ログイン証明書が含まれている場合には、ログイン証明書を取り出し、ステップ２２０４以下を実行する。ステップ２２０４では、ブラウザプログラム１２５ｂからの前記要求がログアウト要求であるかどうかを調べる。本実施の形態では、前記データ処理ルーチンは、前記WWWサーバ１１５ｂに格納されている、ある特定のＨＴＭＬファイルの転送を要求することを、ログアウト要求として解釈する。ログアウト要求である場合には、ログアウト処理を実行し（ステップ２２１７）、ステップ２２０１に戻る。ログアウト要求でなかった場合には、前記WWWサーバプログラム１１５ｂに前記要求を転送する。次に、前記WWWサーバプログラム１１５ｂからＨＴＭＬファイルを受信する。ステップ２２０７で、前記ＨＴＭＬファイルにアクセス権利が設定されているかどうかを調べ、アクセス権利が設定されていなければ、ステップ２２１２で、前記ＨＴＭＬファイルを前記ブラウザプログラム１２５ｂに送信する。一方、アクセス権利が設定されている場合には、ステップ２２０８に移行し、ログイン処理ルーチン２０００をコールし、ログイン処理を行う。次に、ステップ２２０８のログイン処理が成功したかどうかを調べ、ログインに失敗した場合には、エラーメッセージを前記ブラウザプログラム１２５ｂに転送し、ステップ２２０１に戻る。一方、ログインに成功した場合には、ステップ２２１０で、前記アクセス権利確認ルーチン２３００をコールし、ユーザーが前記ＨＴＭＬファイルに対するアクセス権利を持つかどうかを調べる。アクセス権利を持つ場合には、前記ＨＴＭＬファイルを前記ブラウザプログラム１２５ｂに送信し（ステップ２２１２）、ステップ２２０１に戻る。一方、アクセス権利を持たない場合には、前記ＨＴＭＬファイルからエラーメッセージファイルのＵＲＬを取り出し（ステップ２２１３）、前記WWWサーバプログラム１１５ｂにエラーメッセージファイルの転送を要求する（ステップ２２１４）。次に、ステップ２２１５で、前記WWWサーバプログラム１１５ｂからエラーメッセージファイルを受信し、前記ブラウザプログラム１２５ｂに前記エラーメッセージファイルを転送する（ステップ２２１６）。ファイルの転送が終了するとステップ２２０１に戻る。

【０１０８】ログイン処理ルーチン２０００、およびログアウト処理ルーチン２１００は、前記アクセス権利設定プログラム１２５ｃのログイン処理ルーチン１１００、ログアウト処理ルーチン１３００と同じ処理を行うため、ここでは説明を省略する。

【０１０９】次に、図１５を参照して、前記アクセス権利確認ルーチン２３００の動作フローについて説明する。アクセス権利確認ルーチン２３００は、前記WWWサーバプログラム１１５ｂから受信したＨＴＭＬファイルにユーザーがアクセスする権利を持つかどうかを前記アクセス権利判定プログラム１４５ｂに確認するためのものである。

【０１１０】まず、ステップ２３０１で、アクセス権利が設定されたＨＴＭＬファイルから、開示先リストを取り出す。次に、ステップ２３０２で、アクセス権利を持つかどうかを判定するため、前記開示先リストを前記アクセス権利判定プログラム１４５ｂに送信する。次に、ステップ２３０３で、アクセス権利判定プログラム１４５ｂから判定結果を受信し、処理を終了する。

【０１１１】次に、図７、１６から１９を参照して、前記アクセス権利判定プログラム１４５ｂについて説明する。

【０１１２】まず、図７を参照して、前記アクセス権利判定プログラム１４５ｂのモジュール構成について説明する。

【０１１３】図７において、前記アクセス権利判定プログラム１４５ｂは、ログイン処理ルーチン３１００と、アクセス権利判定ルーチン３２００と、ログアウト処理ルーチン３３００とを含んで構成される。

【０１１４】次に、図１６を参照して、前記アクセス権利判定プログラム１４５ｂの動作フローについて説明する。

【０１１５】まず、アクセス権利判定プログラム１４５ｂは、ステップ３００１で、前記データ中継処理プログラム１３５ｂや前記アクセス権利設定プログラム１２５ｃからのアクセスを待ち受ける。（以降、アクセス権利判定プログラム１４５ｂに対してアクセスを行う、前記データ中継処理プログラム１３５ｂや前記アクセス権利設定プログラム１２４ｃをクライアントと総称する。）アクセス要求を受信すると、ステップ３００２で、その要求がログイン要求であるかどうかを調べる。ログイン要求の場合には、ログイン処理を行い、ステップ３００１で、クライアントからの要求待ち状態に戻る。ログイン要求でない場合には、ステップ３００３で、その要求がアクセス権利判定要求であるかどうかを調べる。アクセス権利判定要求の場合には、アクセス権利判定処理を行い、ステップ３００１に戻る。アクセス権利判定要求でない場合には、ステップ３００４で、ログアウト要求かどうかを調べる。ログアウト要求の場合には、ログアウト処理を行い、ステップ３００１に戻る。ログアウト要求でない場合には、ステップ３００１に戻る。

【０１１６】次に、図１７を参照して、前記ログイン処

理ルーチン３１００の動作フローについて説明する。ログイン処理ルーチン３１００は、アクセスを行うユーザーを特定するためのものである。

【０１１７】まず、ステップ３１０１で、クライアントからユーザーＩＤを取得する。次に、パスワード情報ファイルから、ユーザーのパスワード情報を読み込み、ユーザー認証処理を行う。ステップ３１０４で、ユーザー認証処理が成功したかどうかを調べ、成功した場合には、新しいログイン証明書を発行する（ステップ３１０５）。一方、ユーザー認証処理が失敗した場合には、ステップ３１０６に移行し、３回続けて失敗するまでは、ステップ３１０１～ステップ３１０４の処理を繰り返すように制御する。

【０１１８】次に、図１８を参照して、前記アクセス権利判定ルーチン３２００の動作フローについて説明する。アクセス権利判定ルーチン３２００は、ログインしているユーザーが、前記クライアントから送信されてきた開示先リストの条件に適合するかどうかを判定するためのものである。

【０１１９】まず、ステップ３２０１で、クライアントがログイン証明書を持っているかどうかを調べる。ログイン証明書を持っている場合には、ステップ３２０２で、そのログイン証明書が有効かどうかを調べる。ログイン証明書が有効であった場合には、ステップ３２０５以下を実行する。一方、ステップ３２０１でログイン証明書を持っていなかった場合や、ステップ３２０２でログイン証明書が有効でなかった場合には、ログイン処理を行い、ログイン処理が失敗した場合には、そのまま処理を終了する。ログインに成功すると、ステップ３２０５に移行し、ログインしたユーザーのユーザーＩＤ情報を読み込む。次に、クライアントから開示先リストを受信し（ステップ３２０６）、開示先リストの条件を、ログインしているユーザーが満足するかどうかを調べる（ステップ３２０７）。ユーザーが条件を満足する場合には、クライアントに「アクセス権あり」を通知し（ステップ３２０９）、処理を終了する。一方、ユーザーが条件を満足しない場合には、クライアントに「アクセス権なし」を通知し（ステップ３２１０）、処理を終了する。

【０１２０】なお、本実施の形態では、前記アクセス権利判定プログラム１４５ｂは既に無効化されたログイン証明書を保持しており、前記ログイン証明書が、既に無効化されたログイン証明書と一致する場合や、前記ログイン証明書の発行日時を記録するための領域５０３に記述されている値が、現在時刻から１日以上古い値である場合や、前記ログイン証明書のアクセス回数を記録するための領域５０４に記述されている値が、１００を超えている場合や、前記ログイン証明書の最終アクセス時刻を記録するための領域５０５に記述されている値が、現在時刻から１時間以上古い値である場合には、当該ログイン証明書は無効であると判断する。

【０１２１】また、前記クライアント情報処理装置１２（図１参照）から、前記アクセス権利判定装置１４（図１参照）に、ユーザーの属性情報を転送するに際し、クライアント情報処理装置１２において、当該属性情報を予め定められた情報を暗号鍵として暗号化した状態で送信することができる。この場合、上記暗号鍵に対応する復号鍵を前記アクセス権利判定装置１４に予め格納しておき、当該復号鍵を用いて前記暗号化された属性情報を復号化する復号機能を前記アクセス権利判定プログラム１４５ｂ（図１参照）に設けておく。前記アクセス権利判定装置１４において、受信したユーザーの属性情報を前記復号機能により復号化した属性情報が、共有ファイルに付加されている開示先リストが示す条件を満たす否かによって、アクセスする権利の有無を判定することができる。

【０１２２】次に。図１９を参照して、前記ログアウト処理ルーチン３３００の動作フローについて説明する。ログアウト処理ルーチン３３００は、ログインしているユーザーがアクセスを終了することを宣言するためのものである。

【０１２３】まず、ステップ３３０１で、ログイン証明書が有効か否か、すなわち、ログイン証明書が既に無効化されているかどうかを調べる。

【０１２４】既に無効化されたログイン証明書であった場合には、処理を終了する。

【０１２５】一方、未だ無効化されていないログイン証明書であった場合には、当該ログイン証明書を無効化されたログイン証明書として保持してログイン証明書を無効化（ステップ３３０２）し、処理を終了する。

【０１２６】

【発明の効果】以上説明したように、本発明によれば、ＨＴＭＬファイルに付加された開示先リストを基にしてアクセス制御を行うため、ＷＷＷサーバに対して特別な権利を持たない情報作成者でもアクセス権を容易に設定することができる。。

【０１２７】また、本発明によれば、アクセス権利判定装置がユーザーの属性情報を一括して管理し、アクセス制御に関する情報の変更は、ＨＴＭＬファイルに付加された開示先リストを変更するのではなく、アクセス権利判定装置が管理しているユーザーの属性情報を変更することによって行うことができる。従って、アクセス制御に関する情報の変更が容易に行うことができる。

【０１２８】さらに、本発明によれば、ＷＷＷサーバが持っているアクセス制御機能を使用せず、データ中継処理プログラムがアクセス制御を行うことができる。このため、さまざまなＷＷＷサーバが利用されている環境においても、システム全体としては同一の方法でアクセス制御を行うことができる。

【０１２９】そして、本発明によれば、最初のログイン

時にログイン証明書を発行し、当該ログイン証明書を使用して以降のアクセスにおけるユーザーを特定することができる。このため、情報が複数のWWWサーバに跨っている場合でもシステム全体として一度ログインするだけで、アクセスする権利を持っているページのすべてにアクセスすることが可能となる。

【図面の簡単な説明】

【図１】　本発明の一実施形態が適用されたファイル共有システムの概略構成図である。

【図２】　ユーザーＩＤ情報ファイル１４５ｄの内容の一例を示す図である。

【図３】　共有グループ情報ファイル１４５ｅの内容の一例を示す図である。

【図４】　ＨＴＭＬファイル、アクセス権利が設定されたＨＴＭＬファイル、アクセス制御ヘッダの一例を示す図である。

【図５】　アクセス権利設定プログラム１２５ｃの動作フローを示した図である。

【図６】　アクセス権利設定プログラム１２５ｃのモジュール構成を表した図である。

【図７】　アクセス権利判定プログラム１４５ｂのモジュール構成を表した図である。

【図８】　データ中継処理プログラム１３５ｂのモジュール構成を表した図である。

【図９】　ログイン証明書の構成の一例を示す図である。

【図１０】　アクセス権利設定プログラム１２５ｃのログイン処理ルーチン１０００の動作フローを示した図である。

【図１１】　アクセス権利設定プログラム１２５ｃのログアウト処理ルーチン１１００の動作フローを示した図である。

【図１２】　アクセス権利設定プログラム１２５ｃのアクセス権利設定ルーチン１２００の動作フローを示した図である。

【図１３】　アクセス権利が設定されたＨＴＭＬファイルを、サーバ情報処理装置１１とクライアント情報処理装置１２との間で送受する場合に、本実施の形態の各プログラム間で送受されるデータのフローの概略を示した図である。

【図１４】　データ中継プログラム１３５ｂのデータ中継処理ルーチン２２００の動作フローを示した図である。

【図１５】　データ中継プログラム１３５ｂのアクセス権利確認ルーチン２３００の動作フローを示した図である。

【図１６】　アクセス権利判定プログラム１４５ｂの動作フローを示した図である。

【図１７】　アクセス権利判定プログラム１４５ｂのログイン処理ルーチン３１００の動作フローを示した図である。

【図１８】　アクセス権利判定プログラム１４５ｂのアクセス権利判定ルーチン３２００の動作フローを示した図である。

【図１９】　アクセス権利判定プログラム１４５ｂのログアウト処理ルーチン３３００の動作フローを示した図である。

【図２０】　アクセス権利が設定されたＨＴＭＬファイルを、アクセスする権利を持つユーザーが閲覧しようとする場合に表示される、画面の一例である。

【図２１】　アクセス権利が設定されたＨＴＭＬファイルを、アクセスする権利を持たないユーザーが閲覧しようとする場合に表示される、画面の一例である。

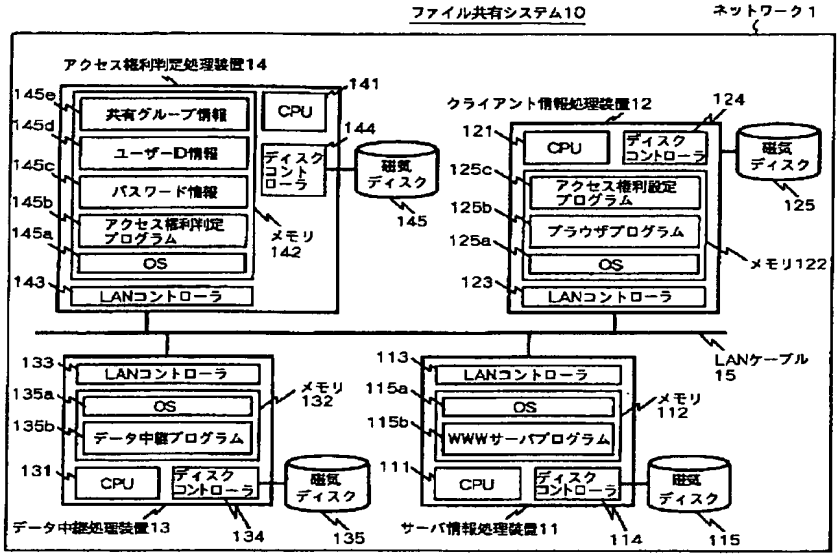
【図２２】　アクセス権利が設定されたＨＴＭＬファイルを、アクセスする権利を持たないユーザーが閲覧する場合に表示される、エラーメッセージファイルの一例である。

【符号の説明】

１…ネットワーク、１０…ファイル共有システム、１１…サーバ情報処理装置、１２…クライアント情報処理装置、１３…データ中継処理装置、１４…アクセス権利判定処理装置、１１１…ＣＰＵ（中央演算処理装置）、１１２…メモリ、１１３…ＬＡＮコントローラ、１１４…ディスクコントローラ、１１５…磁気ディスク、１１５ａ…ＯＳ(オペレーティングシステム)、１１５ｂ…ＷＷＷサーバプログラム、１２１…ＣＰＵ（中央演算処理装置）、１２２…メモリ、１２３…ＬＡＮコントローラ、１２４…ディスクコントローラ、１２５…磁気ディスク、１２５ａ…ＯＳ（オペレーティングシステム）、１２５ｂ…ブラウザプログラム、１２５ｃ…アクセス権利設定プログラム、１３１…ＣＰＵ（中央演算処理装置）、１３２…メモリ、１３３…ＬＡＮコントローラ、１３４…ディスクコントローラ、１３５…磁気ディスク、１３５ａ…ＯＳ（オペレーティングシステム）、１３５ｂ…データ中継処理プログラム、１４１…ＣＰＵ（中央演算処理装置）、１４２…メモリ、１４３…ＬＡＮコントローラ、１４４…ディスクコントローラ、１４５…磁気ディスク、１４５ａ…ＯＳ（オペレーティングシステム）、１４５ｂ…アクセス権利判定プログラム、１４５ｃ…パスワード情報、１４５ｄ…ユーザーＩＤ情報、１４５ｅ…共有グループ情報、２００…ログイン証明書、３００…ＨＴＭＬファイル、４００…アクセス権利が設定されたＨＴＭＬファイル、４１０…アクセス制御ヘッダ。

【図１】

図1



【図２】

図2

ＩＤ情報 145d

	カテゴリ	データ	コード
1	生年月日	19900101	-
2	氏　名	復号次郎	-
3	性　別	男性	1
4	氏名コード	677991234	-
5	事業所	システム研究所	676
6	部	第四部	04
7	課	安全課	402
8	職名	主任	5
9	分野	セキュリティ	X5
10	出身地	神奈川	24

【図３】

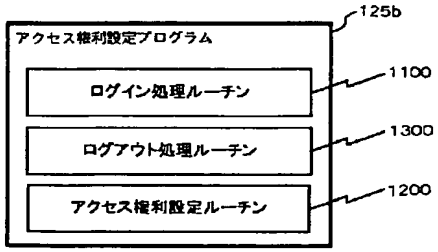
図3

グループ名称	共有グループ情報	作成者	作成日時
本社資材	5C=001^6C=11	001111234	1997.3.21
大阪資材	5C=101^6C=11	101115678	1997.3.21
本社営業	5C=001^6C=21	001210123	1997.4.1
大阪営業	5C=101^6C=21	101214567	1997.4.1
福岡営業	5C=103^6C=21	103218901	1997.4.1
西日本営業	0G=大阪営業,0G=福岡営業	001210001	1997.4.1

145e

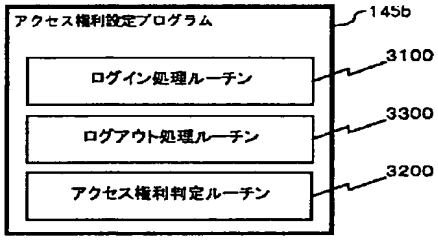
【図６】

図6



【図７】

図7



【図４】

図4

(a)

300

```
<HTML>
<HEAD><TITLE>Sales Information</TITLE></HEAD>
<BODY>
<IMG SRC="image/graph.gif"><P>
(営業機密，取り扱い注意)
当月の販売実績
  東京支店：124
  大阪支店：456
顧客情報
  暗号太郎 Tel:123－4567
</BODY>
</HTML>
```

(b)

410 400

```
<!- GroupAcessControl Version1.0
  OWNER="677991234",
  DATE="28 Sep 1997 18:12:35 +0900",
  ACL="9wLhsFDFevr0zJ9SoHYuy/EPfi0Gr0zJ",
  ERROR="URL=http://www.gac.co.jp/error.html",
  SERVER="ads.gac.co.jp"
->
<HTML>
<HEAD><TITLE>Sales Information</TITLE></HEAD>
<BODY>
<IMG SRC="image/graph.gif"><P>
(営業機密，取り扱い注意)
当月の販売実績
  東京支店：124
  大阪支店：456
顧客情報
  暗号太郎 Tel:123－4567
</BODY>
</HTML>
```

420

(c) アクセス制御ヘッタ410

411 412 413 414 415 416

```
<!- GroupAcessControl Version1.0
  OWNER="677991234",
  DATE="28 Sep 1997 18:12:35 +0900",
  ACL="9wLhsFDFevr0zJ9SoHYuy/EPfi0Gr0zJ",
  ERROR="URL=http://www.gac.co.jp/error.html",
  SERVER="ads.gac.co.jp"
->
```

【図８】

図8

135b

データ中継処理プログラム

- ログイン処理ルーチン 2000
- ログアウト処理ルーチン 2100
- データ中継ルーチン 2200
- アクセス権利確認ルーチン 2300

【図９】

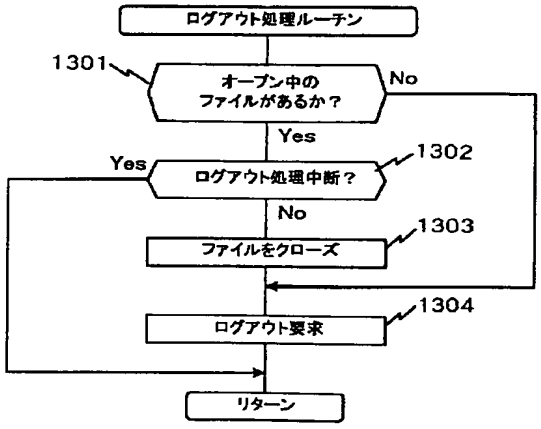
図9

200 ログイン証明書

6789	証明書識別番号 201
677991234	ユーザーID 202
28 Sep 1997 12:00:00 +9:00	証明書発行日時 203
25	アクセス回数 204
28 Sep 1997 18:12:35 +9:00	最終アクセス日時 205

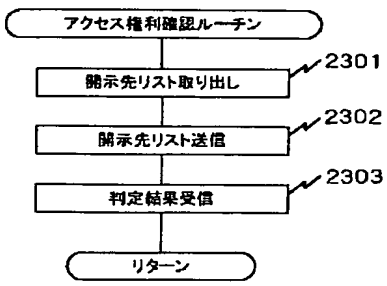
【図１１】

図11



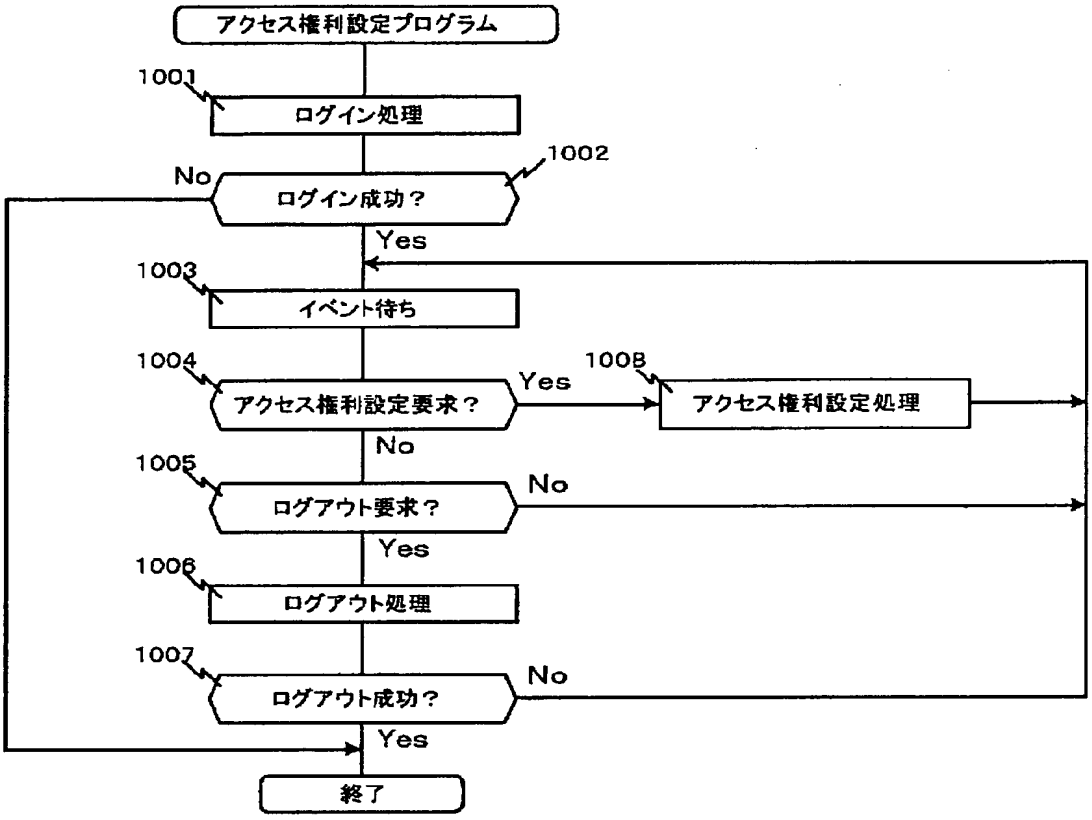
【図１５】

図15



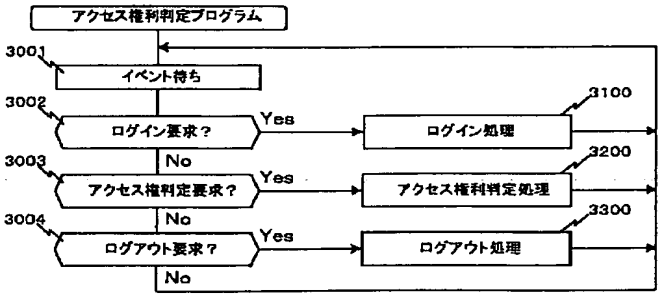
【図５】

図5



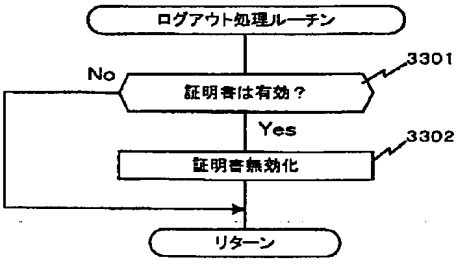
【図１６】

図16



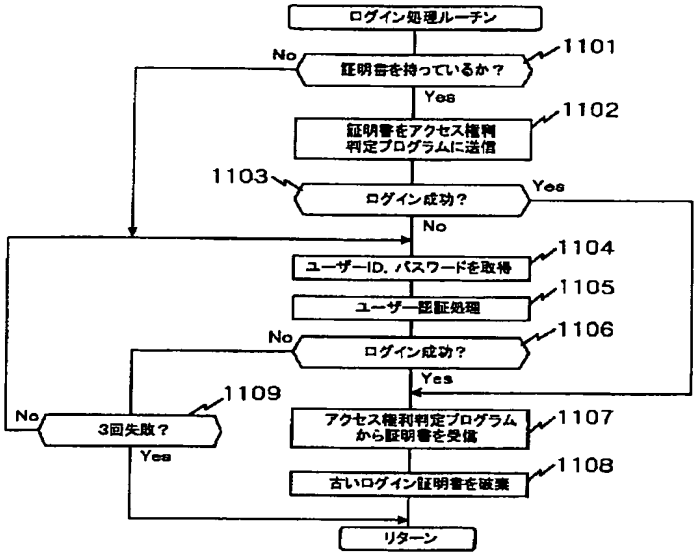
【図１９】

図19



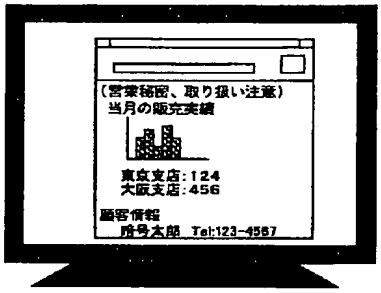
【図１０】

図10



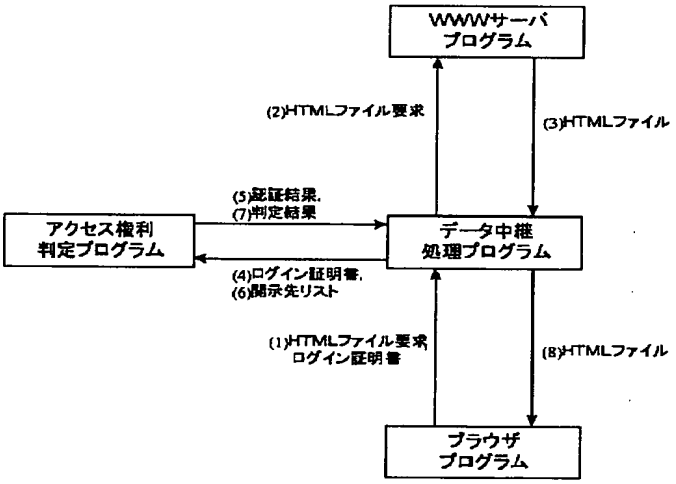
【図２０】

図20



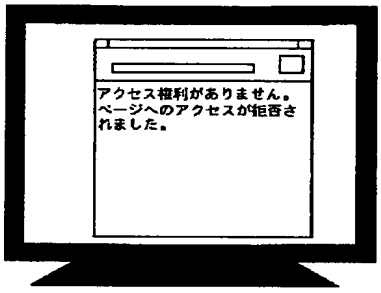
【図１３】

図13



【図２１】

図21



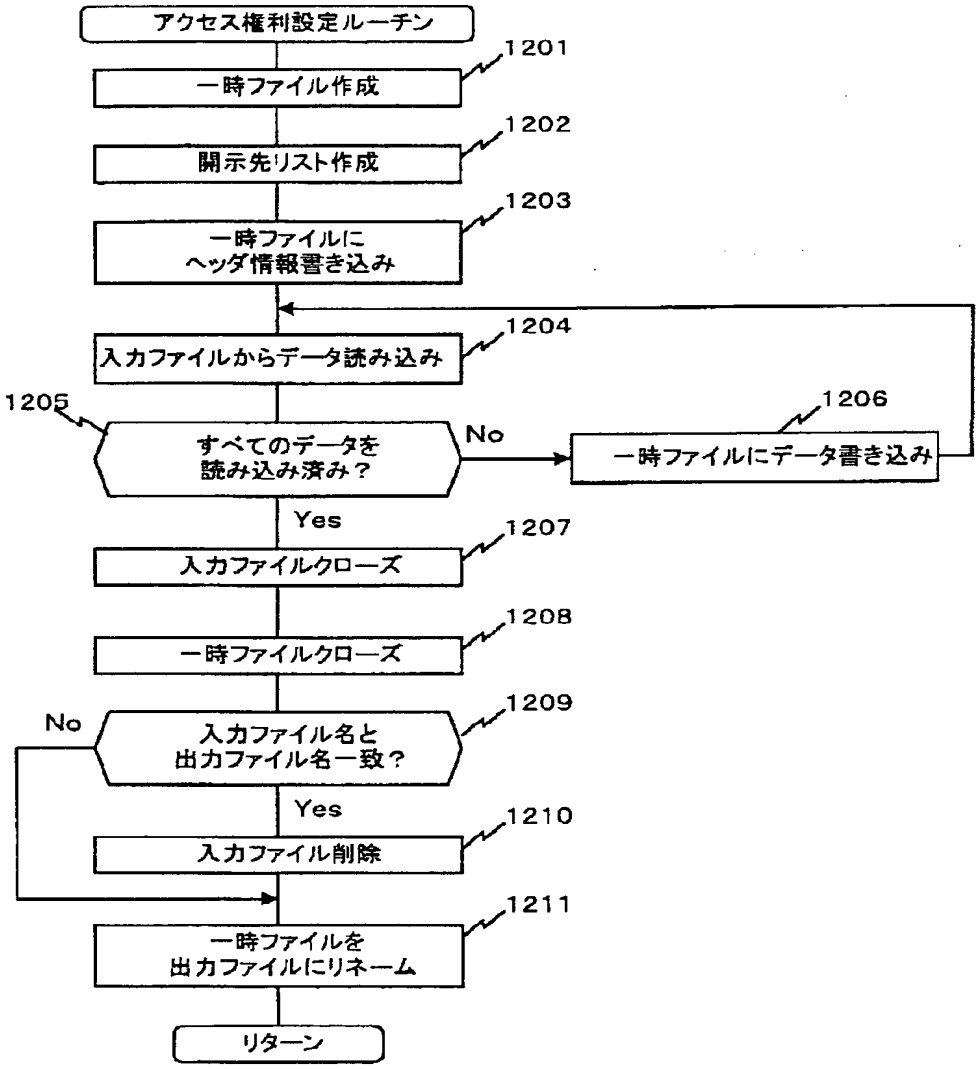
【図２２】

図22

```
<HTML>
<HEAD><TITLE>Access Denied</TITLE></HEAD>
<BODY>
アクセス権利がありません。
ページへのアクセスが拒否されました。
</BODY>
</HTML>
```

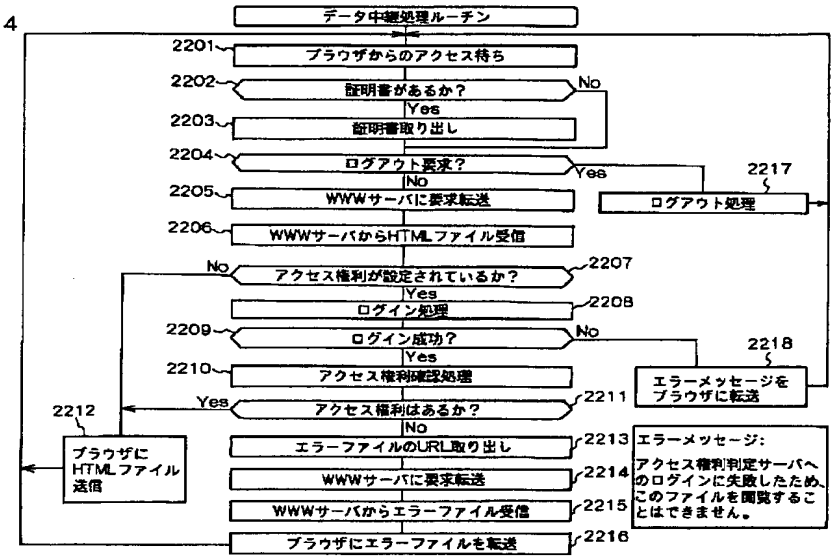
【図１２】

図12


アクセス権利設定ルーチン
1201
一時ファイル作成
1202
開示先リスト作成
1203
一時ファイルに
ヘッダ情報書き込み
1204
入力ファイルからデータ読み込み
1205
すべてのデータを
読み込み済み？
No
1206
一時ファイルにデータ書き込み
Yes
1207
入力ファイルクローズ
1208
一時ファイルクローズ
No
1209
入力ファイル名と
出力ファイル名一致？
Yes
1210
入力ファイル削除
1211
一時ファイルを
出力ファイルにリネーム
リターン

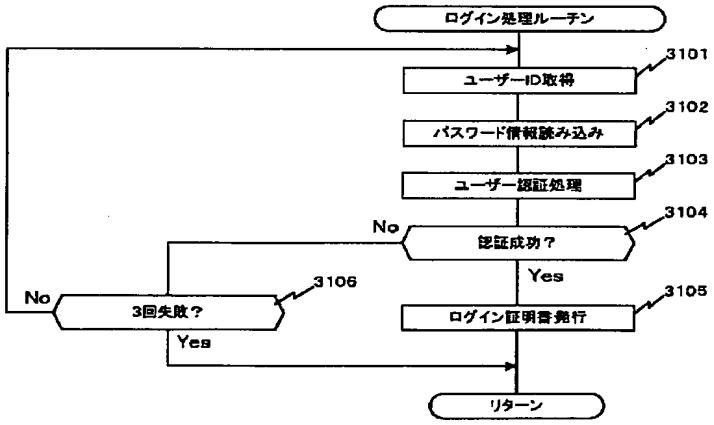
【図１４】

図14



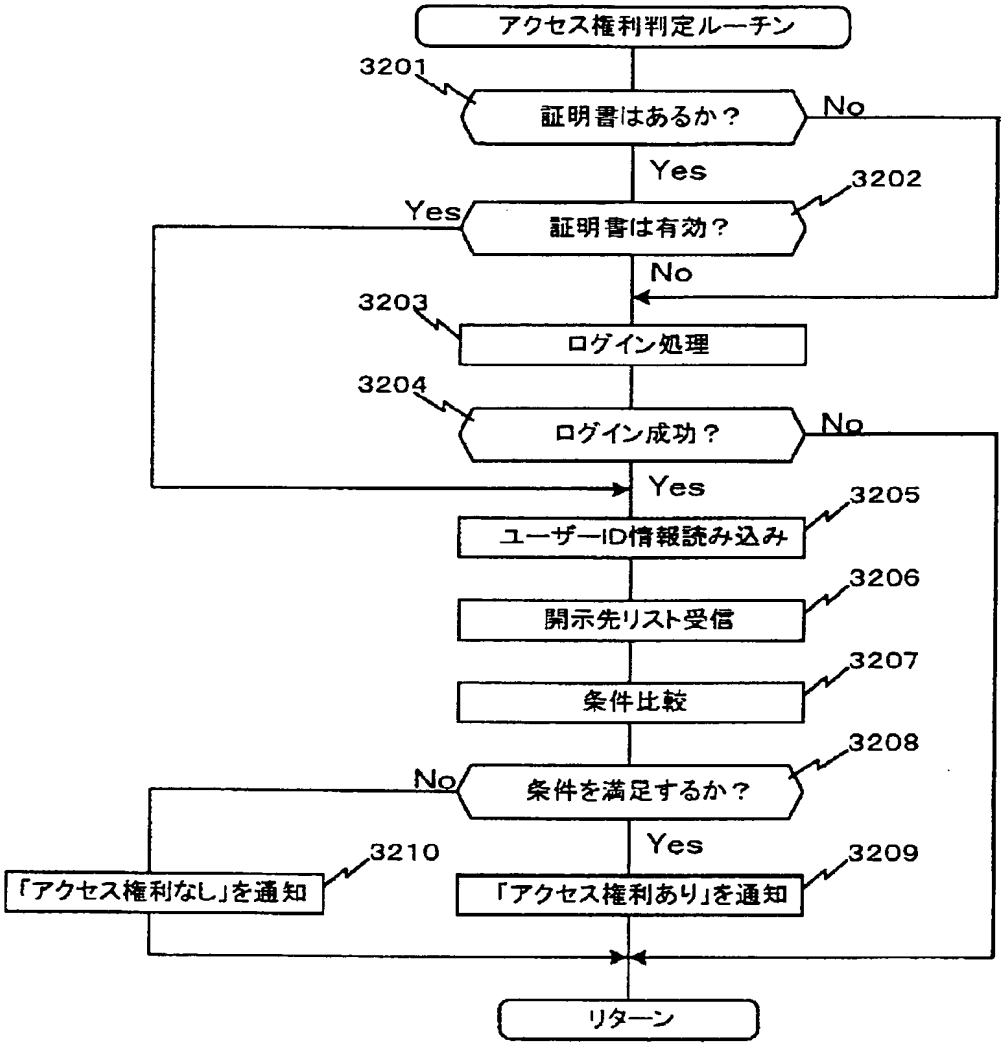
【図１７】

図17



【図１８】

図18



フロントページの続き

(72)発明者　柴田　利幸
東京都品川区南大井六丁目26番３号　株式会社日立情報ネットワーク内

(72)発明者　今村　友彦
東京都品川区南大井六丁目26番３号　株式会社日立情報ネットワーク内